PURPOSE

To establish requirements for training Michigan Department of Health and Human Services (MDHHS) workforce members regarding the secure use of information, systems, and related assets.

REVISION HISTORY

Issued: 1/01/2020.
Next Review: 1/01/2021.

DEFINITIONS

Confidential Information

Sensitive information wherein unauthorized disclosure could cause serious financial, legal, or reputational damage to an agency or the state of Michigan (SOM). Confidential data may include personally identifying information (PII) or confidential non-public information that relates to an agency's business.

Criminal Justice Information (CJI)

Federal Bureau of Investigation (FBI) provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data.

Electronic Protected Health Information (ePHI)

Protected Health Information transmitted or maintained in electronic form.

Federal Tax Information (FTI)

Information that consists of federal tax returns and return information (and information derived from it) covered by the confidentiality protections of the Internal Revenue Code (IRC). FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the Internal Revenue Service (IRS).

Personally Identifiable Information (PII)

Any information about an individual maintained by an agency with respect to, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information that can be used to distinguish or trace an individual's identity (such as name, Social Security Number, date and place of birth, mother's maiden name, biometric records) including any other personal information linked or linkable to an individual.

Protected Health Information (PHI)

Individually identifiable health related information collected by a HIPAA covered entity or component and transmitted by, or maintained in, electronic or any other form or medium.

SSA-Provided Information

Confidential information provided by the Social Security Administration (SSA).

Workforce Member

Includes full and part-time employees, affiliates, associates, students, volunteers, contractors, and staff from third party entities.

POLICY

MDHHS is committed to establishing an information security-aware culture to help protect its information assets. To support this goal, the department must develop and implement a security awareness training program for all workforce members entrusted with access to confidential and sensitive records and information.

In compliance with Department of Technology, Management and Budget (DTMB) 1340.00, Information Technology Information Security Policy, MDHHS must ensure implementation of all moderate baseline security controls catalogued in the National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations (Revision 4) from the NIST Computer Security Resource Center. This policy sets forth requirements from the security awareness and training [AT] family of NIST controls, managed by MDHHS in accordance with DTMB 1340.00.030.01, Security Awareness and Training Standard. MDHHS must review this policy annually.

Where applicable, this policy requires compliance with other federal and state laws, rules and regulations, policies, standards, or other guidelines, including but not limited to the following:

- Centers for Medicare and Medicaid Services (CMS) Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges (MARS-E).
- Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security policy.
- Internal Revenue Service (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies and Entities.
- Social Security Administration (SSA) Technical System Security Requirements (TSSR).
- U.S. Department of Health and Human Services Health Insurance Portability and Accountability Act (HIPAA), 45 CFR Part 160 and Part 164, Subparts A and C.

Security Awareness Training [AT-2]

Prior to granting system access, MDHHS must provide basic security awareness training to all workforce members as part of new hire orientation. Training must take place annually thereafter, or sooner as required by system, organizational and/or compliance changes.

Training content must:

- Provide a basic understanding of information security.
- Leverage various forms of media, including, but not limited to, on-site training, during new hire orientation, online security and privacy training modules managed within the department, and SOM enterprise online training.
- Explain threats and vulnerabilities that place information at risk in the workplace.
- Detail, in separate training modules, specific requirements applicable to workforce members with access to certain categories of federally controlled information, developed,

administered, and documented, including but not limited to the following:

- For SSA-provided information, Section 5.10 Security Awareness Training and Employee Sanctions and Section 5.11, Contractors of Electronic Information Exchange Partners as detailed in the SSA TSSR currently in force.
- For FTI, Sections 6.2,6.3, and 9.3.2 of IRS Publication 1075.
- For CJI, Section 5.2 Policy Area 2 of the FBI Criminal Justice Information Services (CJIS) Security Policy.

- Describe actions and behaviors necessary to maintain a secure environment.
- Promote a sense of personal responsibility for effective security, irrespective of position, grade, or level of access.

Insider Threat [AT-2(2)]

MDHHS security awareness training must include guidelines for recognizing indicators for potential insider threats and procedures to communicate concerns, potential violations, and reporting instances of suspected wrongdoing to management.

Role-Based Training [AT-3]

MDHHS must provide role-based security-related training to workforce members with assigned security roles and responsibilities before granting access to information systems or performing assigned duties, when required by system changes, and during annual refresher training.

Training Records and Recordkeeping [AT-4]

MDHHS must:

- Document and monitor individual security awareness training activities, including basic security awareness training and role-specific information system security training.
- Retain training records for a minimum of five years.

ROLES AND RESPONSIBILITIES

The MDHHS security officer and privacy officer must determine roles and responsibilities for Compliance and Data Governance Bureau personnel to support implementation of this policy.

MDHHS workforce members are responsible for:

- Completing new hire and refresher security awareness training within timeframes of this policy.
- Reading, understanding, and complying with agency and department security policies and procedures.

ENFORCEMENT

Violations of this policy or failure to implement provisions of this policy may result in disciplinary action up to and including termination, civil litigation, and/or criminal prosecution.

State Standards/Regulations

DTMB Administrative Guide.

DTMB/Work Resources/Policies, Standards and Procedures/IT Technical Policies, Standards and Procedures.

1340.00.030.01 Security Awareness and Training Standard.

CONTACT

For additional information concerning this policy, contact the MDHHS Compliance and Data Governance Bureau at MDHHSPrivacySecurity@michigan.gov.